EXHIBIT L

Frequently-Asked Questions about RealSecure

Last updated: May 30, 1997, 4:00 pm

TABLE OF CONTENTS

Q1: What is RealSecure?

Q2: What kinds of network events does RealSecure recognize?

Q3: What types of protocols can RealSecure see and decode?

Q4: How does RealSecure work?

Q5:How does RealSecure respond to attacks?

Q6: What platforms can RealSecure run on?

Q7: What networks can RealSecure monitor?

Q8: What Ethernet cards does RealSecure support?

Q9: What are the recommended specifications required for a host to run RealSecure?

Q10: How is RealSecure deployed across the enterprise network?

Q11: How do the RealSecure engines communicate with the RealSecure management console?

Q12: What authentication scheme do you use? What encryption scheme do you use?

Q13: How does RealSecure differ from a firewall? Don't they do the same things?

Q14: Do I need firewalls if I have RealSecure?

Q15: What do I have to do to my network to run RealSecure?

Q16: Will RealSecure run on a switched network?

Q17: How much delay does RealSecure add to the network?

Q18: How much additional traffic does RealSecure add to the network?

Q19: Can RealSecure be completely transparent? Must RealSecure have an IP address?

Q20: Can RealSecure detect unauthorized activity in a Windows networking environment?

Q21: Can RealSecure play back logged traffic data at a later date?

Q22: How can I configure RealSecure specifically for my network?

Q23: Can RealSecure be used for URL blocking?

Q24: Can I customize RealSecure's response to a network event?

Q25: Can RealSecure flag SSH and SSL traffic?

Q26: Can RealSecure log and flag the type and size of traffic or network service?

Q27: How does RealSecure detect a SYN flood?

Q28: How many RealSecure engines can a RealSecure console manage at one time?

Q29: Can RealSecure data be analyzed with a decision support system?

Q30: How are updates handled? Can an administrator upgrade fifty engines across an enterprise (for example) without losing configuration settings?

Q31: Can multiple RealSecure engines run on a single host with multiple adapter cards?

Q32: This product gathers a lot of information about my network. How should the RealSecure host be configured in order to protect this product from misuse?

Q33: How do I get a copy of RealSecure?

Q34: Whom do I contact for technical support?

Q35: Whom do I contact with product suggestions?

Q1: What is RealSecure?

A: RealSecure(TM) is a real-time, automated attack recognition and response system. It sits on your network, monitoring the network traffic stream looking for attacks and unauthorized access attempts. When RealSecure detects an attack, it can respond in a variety of ways, including logging the connection, notifying the network administrator, and killing the connection automatically.

Back To Top

Q2: What kinds of network events does RealSecure recognize?

A: RealSecure recognizes two types of network occurrences:

Attacks
Network activity patterns indicating that someone may be engaged in unauthorized or undesirable activity involving the systems and/or data on your network. Examples of these include SATAN scans, ping floods, WinNuke packets, SYN floods, IP half scans, and attempts to obtain unauthorized root access.

Sessions
Non-attack network activity that may be of interest to the network administrator. Examples of these include HTTP activity (who's surfing the net and where they're going), analysis of access to Windows shares (e.g., connections from engineering to accounting), and e-mail session decoding.

RealSecure is shipped with the most comprehensive set of attack recognition patterns in the industry.

Back To Top

Q3: What types of protocols can RealSecure see and decode?

A: RealSecure can filter and monitor any TCP/IP protocol. The network administrator can configure RealSecure to filter by protocol (TCP, UDP, ICMP), source port, destination port, source IP address, and/or destination IP address. RealSecure can interpret the following network services: web surfing, e-mail, file transfer, remote login, chat, talk and a host of others. The range of services that RealSecure can analyze is extended regularly, so be sure to check the ISS web site at http://web.archive.org/web/19970721183227/http://www.iss.net/ for the latest status.

In addition, RealSecure will soon be able to monitor and decode Microsoft CIFS/SAMBA traffic for Windows networking environments.

Back To Top

Q4: How does RealSecure work?

A: RealSecure is installed on a host having a network adapter card. RealSecure puts the adapter card in promiscuous mode so that it acts like a sniffer and receives all the traffic on the local network segment. If a packet meets the filter criteria currently in force, it is parsed by the decode and attack recognition logic. Each active session is maintained and tracked, so that attack patterns that span many packets can be detected. This way, when an "interesting event" is detected, the appropriate actions can be taken.

RealSecure is completely unobtrusive. It only monitors the local traffic. RealSecure does not add any delay to the network segment.

Back To Top

Q5: How does RealSecure respond to attacks?

A: The actions taken upon detection of an attack or unauthorized activity are determined by the administrator. The administrator may choose from the following options:

- Display a message indicating that the event occurred
- View the session in real-time (or record for later playback)
- Kill the connection automatically by sending a reset packet to each session participant
- E-mail a notification to the administrator
- Execute a user-specified program
- Log the data related to the event for later reporting or playback

Back To Top

Q6: What platforms can RealSecure run on?

A: Currently, RealSecure is supported on the following platforms:

- SunOS 4.1.3 or later
- Linux 1.3.x
- Solaris (SPARC) 2.3 or later

However, RealSecure for Windows NT platforms is currently scheduled to ship in July, 1997.

Back To Top

Q7: What networks can RealSecure monitor?

A: RealSecure currently operates over Ethernet networks only. ISS will be adding support for FDDI and Fast Ethernet in the short term, with support for additional networking topologies to follow.

Back To Top

Q8: What Ethernet cards does RealSecure support?

A: RealSecure will operate over any Ethernet card that is capable of supporting promiscuous mode. Check the documentation for your Ethernet adapter to determine whether your card has this capability.

Back To Top

Q9: What are the recommended specifications required for a host to run RealSecure?

A: SunOS and Solaris: SPARC 5 or better
At least 32 Mbytes of RAM
At least 60 Mbytes of free disk space
Motif installation (Solaris 2.3, 2.4 for GUI)
Ethernet interface connected to the target network

Linux: Pentium 90 MHz. or better
At least 32 Mbytes of RAM
At least 60 Mbytes of free disk space
X-Window system, version 11 or higher for GUI
Ethernet interface connected to the target network

Windows NT: Pentium 90 MHz. or better
At least 32 Mbytes of RAM
At least 60 Mbytes of free disk space
Windows NT 4.0
Ethernet interface connected to the target network.

The configurations listed above assume that the management console and an engine are running on the specified host. If you are running an engine only, then you can reduce the RAM requirements to 16 Mbytes.

Back To Top

Q10: How is RealSecure deployed across the enterprise network?

A: RealSecure uses a distributed architecture. The RealSecure engine performs its filtering and monitoring functions on a given network segment. The RealSecure management console displays and logs the data and acts as a centralized engine management point.

Many RealSecure engines can report to a single management console. As engines detect unauthorized activity they take the appropriate action and then send a message to the management console so that the administrator can see what has happened. Engines can also upload their local log files and databases to the management console periodically, so that the network administrator has a centralized report of network activity.

With regard to placement of RealSecure engines, the best rule is to place a RealSecure engine on each segment where there is critical data to protect or a set of users that should be monitored.

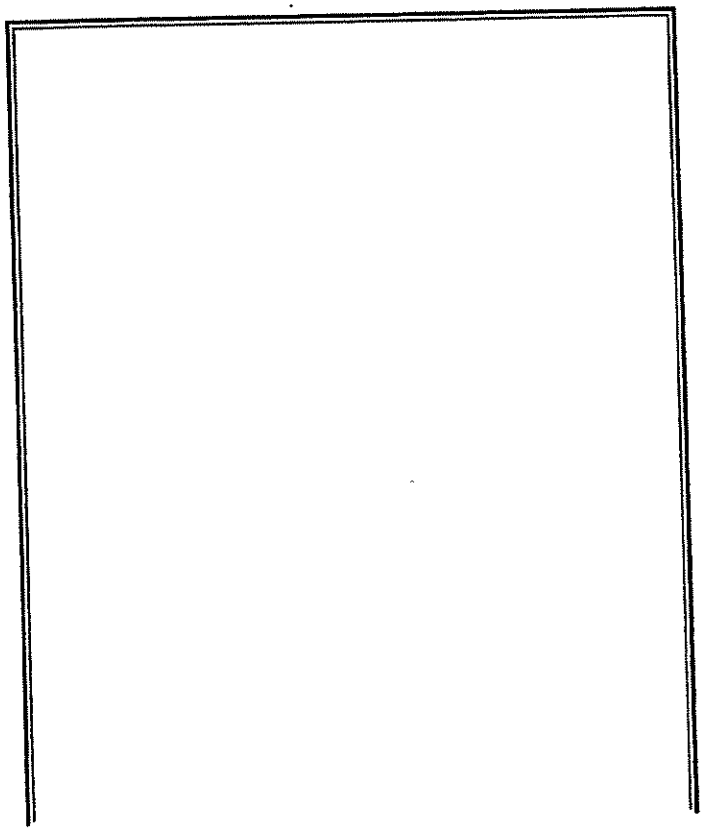
Note that a RealSecure engine will only see the traffic that is on the local network segment. Since routers prevent traffic from being copied to inappropriate segments, several RealSecure engines might be needed for complete coverage of network activity.

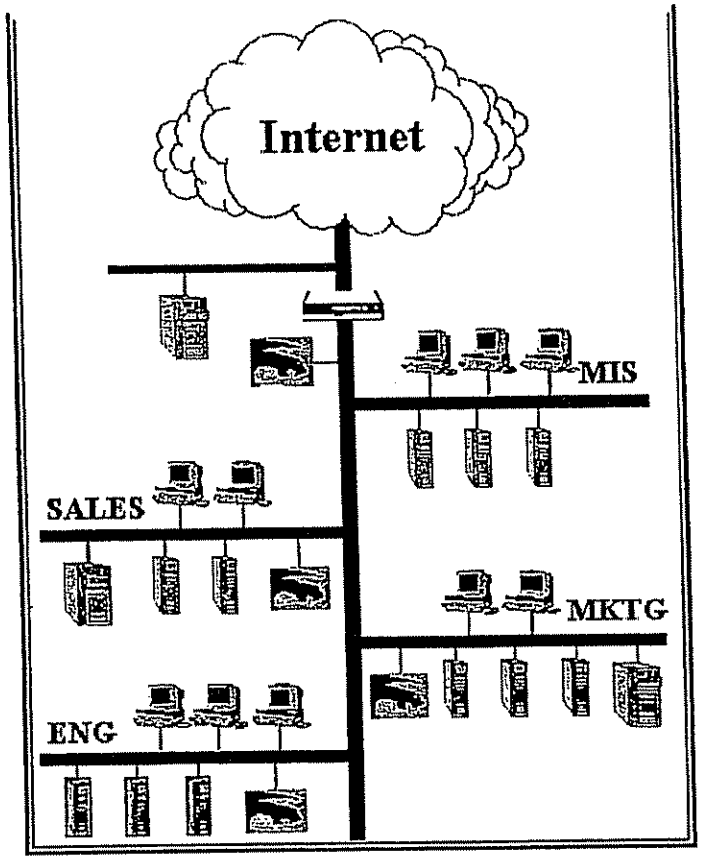
The following figure shows a sample deployment of RealSecure.

- There is a RealSecure engine behind the firewall monitoring the traffic flow on and off the network. This engine will detect unauthorized activity from the Internet. It will also help the administrator detect misconfigurations in the firewall.
  Many companies also place a RealSecure engine outside the firewall in the DMZ, to protect the external web server and to analyze external traffic.
- There is a RealSecure engine on the Sales subnet because this is where the sales database resides.
- The RealSecure engine on the Marketing subnet protects the business plans and marketing strategies on the systems in that department.
- The Engineering subnet also supports a RealSecure engine because the source code archive is kept there.
- All of these engines can report to a single management console. That console might be located on the company's internal network or at a headquarters across the internet or at a Network Operations Center staffed by a service organization.

In this sample deployment, it is also possible to install RealSecure engines on the backbone that would see all the intersegment traffic. However, installing engines on each segment provides two distinct advantages:

- Each engine can be customized for the local segment. For example, the engine on the sales subnetwork can be configured to examine all traffic directed to the sales database.
- Engines on the local segments will detect unauthorized activity that is initiated on that segment, an engineer attempting to gain root access to the source code archive, for example.





Back To Top

Q11: How do the RealSecure engines communicate with the RealSecure management console?

A: Data from the engines to the management console includes:

- Event messages - indications that something interesting has happened. These are passed up to the management console as they occur.
- Raw session data - the keystroke or data content of a session. This information is passed up to the management console as it occurs if the action associated with an event is "View Session".
- Database and log file information. These are sent up to the management console on demand.

Data from the management console to the engines includes:

- Start, stop, and pause commands.
- Changes to filter rules, attack signatures, and event responses.
- Keep-alive checks.

- Software updates.

The engines and the management console communicate using TCP port 590 and UDP ports 900 and 901. Data passed between the systems is encrypted and authenticated.

Back To Top

Q12: What authentication scheme do you use? What encryption scheme do you use?

A: The authentication scheme is a variation of the challenge-handshake authentication protocol. The management console provides a list of the engines that it manages along with a pass phrase used to authenticate data from each engine. Each engine contains a similar list for the management console. When one side wants to send a message to the other, the pass phrase is appended to the data, an MD5 checksum is calculated for the entire data set, and the checksum is attached to the packet (without the pass phrase). The entire message is encrypted and sent out over UDP.

Upon receiving the message, the other side of the connection will decrypt the data field, remove the checksum, attach the pass phrase, calculate an MD5 checksum, and compare with the checksum received. If they match, the message is authenticated.

The current encryption scheme is a fully exportable ISS proprietary encryption method. RealSecure will use a standard encryption method in a subsequent release.

Back To Top

Q13: How does RealSecure differ from a firewall? Don't they do the same things?

A: Firewalls and RealSecure use similar technologies to accomplish different things. Firewalls are *controlling* entities. They enforce general entry and exit rules for an entire network and aren't designed to look for attack patterns. Their main purpose is to keep the wrong kind of traffic off the network and their definition of "wrong kind of traffic" is usually based on IP address or protocol type.

RealSecure is not a product that controls network access. RealSecure does not interfere with the network traffic stream at all. Instead, it allows the traffic to go by and quietly watches for signs of unauthorized activity. RealSecure's definition of "unauthorized activity" is a sophisticated and customizable database of attack signatures.

Think of your network as a high-rise apartment building, the firewall as the doorman, and each RealSecure engine as a guard dog on a specific floor. The doorman is generally pretty good about letting the right people in and keeping the wrong people out. However, a moderately clever criminal will be able to get past the doorman and into the building. The guard dog is better at knowing who's authorized to be on the floor and responding quickly to stop the intrusion.

Back To Top

Q14: Do I need firewalls if I have RealSecure?

A: Absolutely. RealSecure is an essential addition to, but not a replacement for, your firewall security. When firewalls are properly configured, they keep out most undesired traffic. However, in order to provide some level of access, firewalls have tunnels and these tunnels can be exploited by would-be attackers. A good example is FTP. Many companies have an FTP server inside their network and associated tunnels through the firewall to allow access. A common attack is to attempt to gain root access to the FTP server. Once an attacker has access to a system inside the network, other systems become vulnerable. And although the firewall will not stop this type of attack, RealSecure will. By monitoring the traffic stream on the network behind the firewall, RealSecure can detect and terminate attempts to gain root access on the FTP server.

The other unfortunate reality is that firewalls are often misconfigured. A poorly configured firewall offers about as much protection as cheap sunglasses on an August afternoon. Although firewall misconfigurations should be fixed as soon as possible, having RealSecure inside the network can catch much of the undesirable traffic that's leaking through. Even if you choose not to terminate these undesired connections, the sheer number of alarms that RealSecure will generate will quickly indicate that your firewall is not doing its job.

Back To Top

Q15: What do I have to do to my network to run RealSecure?

A: Nothing. You don't have to buy new routers or bridges; you don't have to install any software on your servers; you don't have to reconfigure any devices. RealSecure works with your existing network infrastructure. All you need to do is place a UNIX® or Windows NT® system with an Ethernet card on the segment to be monitored and install RealSecure.

Back To Top

Q16: Will RealSecure run on a switched network?

A: Yes. Right now, this is primarily an issue of deployment.

Network switches (as well as IP switches) break a network into segments. Traffic that is not addressed to a system on a given segment will not be transmitted on that segment by a switch. Therefore, one alternative is to place an engine on each segment that contains critical data that need to be monitored carefully.

There are switches, however, that allow only a single MAC address to be attached to each port. These are usually referred to as "desktop switches". If you have desktop switches, it will

be necessary to deploy a RealSecure engine at a higher level of the network, upstream from the switch, so that the engine will detect traffic between the switch and the rest of the network.

It's also important to note that ISS is working on ways to provide more detailed RealSecure coverage of switched networks.

Back To Top

Q17: How much delay does RealSecure add to the network?

A: None. Unlike firewalls, which often store and evaluate data before forwarding it to the inner network, RealSecure is completely unobtrusive. RealSecure monitors the network traffic, copying packets as needed, but does not alter or delay the traffic at all. The only time that RealSecure will have any impact the traffic flow is when it terminates connections in response to an attack and this won't be noticed, except by the attacker.

Back To Top

Q18: How much additional traffic does RealSecure add to the network?

A: In a standalone configuration (i.e., engine and management console on the same host), RealSecure will add no additional traffic to the network, since all communication between engine and management console takes place on the host.

In a distributed configuration (i.e., engines distributed around the enterprise network reporting data to the management console), the amount of additional traffic will depend on several factors:

- The number and frequency of network events reported from the engine to the management console.
- The frequency of database and log file uploads from the engine to the console.
- The size of the database and log file uploads from the engine to the management console. The administrator may choose not to upload everything, but may want a subset of the stored information instead.

Back To Top

Q19: Can RealSecure be completely transparent? Must RealSecure have an IP address?

A: Yes. RealSecure can be completely transparent. It is possible to monitor a network without the knowledge of the users on the network.

The RealSecure engine requires TCP/IP to communicate with the management console. Consequently, it requires an IP address. This is true even when the engine and management

console are running on the same host.

Back To Top

Q20: Can RealSecure detect unauthorized activity in a Windows networking environment?

A: The next versions (Unix in June 1997, Windows NT in July 1997) will include the ability to decode SAMBA/ CIFS protocols for Windows networking. The product will also include several new attack signatures specific to the Windows networking environment. These will include the ability to detect:

- When one user attempts to copy a password file (.pwl) from a shared volume on a Windows 95 system.
- Remote registry access attempts.
- Null sessions.
- Attempts to read from or write to protected shares.

Back To Top

Q21: Can RealSecure play back logged traffic data at a later date?

A: RealSecure cannot playback logged data as if it were being received from the adapter card. However, network events can be stored in log files and databases for retrieval at a later date. RealSecure provides sophisticated reporting features that allow the administrator to sort and format event data by priority, source address, destination address, or network service over some period of time.

RealSecure also includes the ability to record the raw, binary content of an entire network session. This data is stored in a log file and can be replayed through the management console interface. It is played back exactly as it was received, keystroke for keystroke, so that the administrator can see how the attack or session unfolded.

Back To Top

Q22: How can I configure RealSecure specifically for my network?

A: There are two ways to customize RealSecure.

First, you can add your own filter rules to RealSecure. RealSecure can be instructed to filter on any combination of the following:

- Protocol
- Source IP address
- Destination IP address

- Source port
- Destination port

For example, a network administrator might want to log all traffic to the server that contains the financial data for the corporation. She would do this by adding a filter that would catch all traffic to the IP address of the server.

Second, you can alter the actions that RealSecure takes when an attack or event is detected. These actions include the following:

- Log a summary of the event (date, time, source, target, type of event).
- Log the entire binary content of a session.
- Display a message on the management console about the event.
- Notify the network administrator via e-mail.
- View the session in real-time.
- Kill the connection.
- Execute a user-defined program (UNIX version only).

Back To Top

Q23: Can RealSecure be used for URL blocking?

A: Yes, but in a limited fashion. RealSecure is not designed to be a "network nanny" that enforces appropriate usage policies on a network. Its real function is security.

You can install filters that match certain web sites and you can instruct RealSecure to terminate connections that match these filters. For example, I might install a new filter that terminates all connections from 208.21.4.0 (sexkitten.com) and from port 80 (HTTP). However, RealSecure is not a product that is designed to be used in this manner and you will find that there are other, easier ways of blocking certain URLs on your LAN.

Back To Top

Q24: Can I customize RealSecure's response to a network event?

A: Yes. See question 22.

Back To Top

Q25: Can RealSecure flag SSH and SSL traffic?

A: Yes.

Back To Top

Q26: Can RealSecure log and flag the type and size of traffic or network service?

A: RealSecure can log and flag the type of traffic, but not the size. RealSecure is not designed to monitor or manage the performance of the network segment, but the security.

Back To Top

Q27: How does RealSecure detect a SYN flood?

A: Some of the attacks that RealSecure detects involve more than just a single packet or single protocol type. Some involve variables that can be tuned for your network. SYN Flood is a good example. A SYN Flood is a denial of service attack. When a TCP connection is established, the initiator of the connection (the attacker, in this example) sends a SYN packet to the destination (the target system, in this example). The target system will acknowledge the connection and allocate memory to hold information about the connection. By establishing, but not using, many TCP connections, the attacker can cause the target machine to run out of memory and possibly crash.

RealSecure detects SYN Floods by monitoring the TCP connections that are established and by setting thresholds for the number of outstanding connections on a given machine at a given time. The network administrator may adjust the value of this threshold as appropriate for the network. There are several other attack signatures, like SYN Flood, that have tunable parameters.

Back To Top

Q28: How many RealSecure engines can a RealSecure console manage at one time?

A: There is no hard and fast limitation to the number of engines that can be controlled by a single RealSecure management console. The practical number depends on several factors:

- The system configuration of the host running the management console software.
- The amount of traffic that flows between the engine and the console.
- The number of attacks and events recognized by the engine.

For example, a console managing twenty engines on a busy network with lots of attacks in progress can receive more data than a console managing 100 engines on a quiet network with few attacks and very tight filter rules.

In addition, there is also a human limit as to how many subnetworks can be managed from a single point. Practically speaking, the number of engines that will normally be report to a single console will depend on the geographic and organizational limitations of the controlling organization.

Back To Top

Q29: Can RealSecure data be analyzed with a decision support system?

A: Yes, if the decision support system is capable of reading an ODBC database.

Back To Top

Q30: How are updates handled? Can an administrator upgrade fifty engines across an enterprise (for example) without losing configuration settings?

A: Updates are posted on the ISS web site (http://web.archive.org/web/19970721183227/http://www.iss.net/) and users are notified of the new software via e-mail. The new release can be downloaded and installed at the administrator's convenience. Installation uses built-in file copy capabilities and is as simple as copying a new executable to the appropriate locations.

Since configuration settings (i.e., filter rules, enabled attacks, engines being managed) are saved in separate configuration files, installation of new software will have no effect on the current settings.

Back To Top

Q31: Can multiple RealSecure engines run on a single host with multiple adapter cards?

A: Not at present. There is currently a limit of one RealSecure engine per host. However, this is a feature that will be supported in a subsequent release.

Back To Top

Q32:This product gathers a lot of information about my network. How should the RealSecure host be configured in order to protect this product from misuse?

A: RealSecure is an amazingly powerful tool designed for network administrators. However, it could become a potentially dangerous tool in the wrong hands. It can grab user names, passwords, and even e-mail and file transfer content. Therefore, ISS recommends the following:

- Scan the engine and management console with ISS' Internet Scanner and System Security Scanner (S3) to minimize the system's vulnerability to attack. Use RealSecure on a dedicated host. Do not run any other applications on the system.
- Disable all services except for TCP/IP. The RealSecure engine reads raw data link

packets from the adapter card, but uses TCP and UDP to communicate with the management console.
- Ensure that nothing is listening on any of the ports except for TCP 590 and UDP 900 and 901. These are the ports used for engine-console communication.
- Ensure that root or administrator access to the device is restricted. It would be a good idea if all other logins were disabled.

Back To Top

Q33: How do I get a copy of RealSecure?

A: Download an evaluation copy from the ISS web site at http://web.archive.org/web/19970721183227/http://www.iss.net/. Or, you can call us at 1-800-PROBE-62 (1-800-776-2362).

Back To Top

Q34: Whom do I contact for technical support?

A: You can send e-mail to support@iss.net. Or you can download our tech support FAQ from the ISS web site at http://web.archive.org/web/19970721183227/http://www.iss.net/. Finally, you can call us at 1-800-776-2362 and ask for technical support.

Back To Top

Q35: Whom do I contact with product suggestions?

A: For RealSecure, send an e-mail to the Product Manager, Mark Wood, at mwood@iss.net.

Back To Top

Technical Support: support@iss.net

04/30/97